U.S. General Service Administration

Performance Work Statement (PWS)

For The

Defense Manpower Data Center (DMDC)
Enterprise Information Technology Services II (EITS II)
Indefinite Delivery Indefinite Quantity (IDIQ) Contract

GSA ITSS Order ID No.: ID03180056

Issue Date: 8 February 2019

Revision Date: As listed in Table of Revisions

Table of Revisions

Rev. No.	Rev. Date	Description	Mod No.
01	08/14/19	Added Task 8 Intelligence and Investigations Support, Updated the Deliverable Table, and the Appendices.	01
02	05/29/20	Revise PWS paragraph 5.9.9 to change Subcontract Reporting due date.	03

Performance Work Statement
DMDC Enterprise Information Technology Services (EITS) II IDIQ Contract

1.0 INTRODUCTION

The Defense Manpower Data Center (DMDC) in support of the Office of the Under Secretary of Defense for Personnel & Readiness (OUSD P&R), Defense Human Resource Activity (DHRA) requires information technology services to support IT services and systems serving the Federal Government, the Department of Defense (DOD), Service Members and their beneficiaries.

2.0 BACKGROUND

2.1 The Defense Manpower Data Center (DMDC) supports major programs and initiatives within the Department of Defense (DoD) and maintains the largest archive of personnel, manpower, training, security, and financial data within the DoD. The personnel data holdings, in particular, are broad in scope and date back to the early 1970s, covering all Uniformed Services, all components of the Total Force (Active Duty, Guard, Reserve, and Civilian), and all phases of the personnel life cycle (accessions through separation/retirement). The categories of data archived at DMDC represent significant data holdings and, in most cases, provide the only single source of commonly coded data for the Uniformed Services. This data supports decision making by the Office of the Undersecretary Defense for Personnel and Readiness (OUSD (P&R)), other Office of the Secretary of Defense (OSD) organizations, and a wide variety of customers both within and outside the DoD. DMDC's programs include verifying military entitlements and benefits (e.g., health care, dental, education, and life insurance); managing the DoD Identification (ID) card issuance program; providing identity management for the DoD; employee and Service member travel assistance; personnel and property identification; authentication and access control systems; security clearance, adjudication, and continuous monitoring tools; debt protection for deployed Service members and predatory lending protection for members and their families; personnel evacuation support systems; and assisting military members and their spouses with transition to civilian life. Supporting applications and databases are available to the user community 24 hours per day, seven days per week, with sub-second response time. Any outage can result in disruption of services to DoD beneficiaries as well as potential financial claims from the TRICARE contractors. Additional information about DMDC can be obtained at https://www.dmdc.osd.mil.

2.2 DMDC historically managed programs by lines of business with unique platforms and architectures, limiting the ability to consolidate programs and capabilities to achieve cost savings. In 2017, Under Secretary of Defense for Personnel and Readiness (USD P&R) directed a reorganization of DHRA and DMDC. Under the DMDC Director's direction, DMDC moved to implement a service delivery model with an enterprise-wide architecture to normalize and consolidate legacy applications to enable migration to a virtualized, cloud infrastructure. This transformation of the organization, culture, and programs requires a strategic re-thinking of contracted support and services. To eliminate barriers to standardization, contracts must be aligned to deliver enterprise-wide capabilities vice delivering stand-alone applications and systems.

2.3 The major components of DMDC's IT environment, major programs and software supported by this Performance Work Statement (PWS) are described in Appendices A through L of this PWS. DMDC's portfolio is constantly evolving and growing and as a result, requires development and sustainment support for numerous components, applications, and systems. It is anticipated that during the life of this order DMDC will augment and change tools to improve visualization, usability, speed of delivery of data

and to create a more cost effective footprint. DMDC anticipates that these components, applications and information may change before and during the performance of this contract.

2.4 PROGRAM OVERVIEW & TECHNOLOGY ENVIRONMENT

The major components of DMDC's IT environment, major programs and Commercial-Off-The-Shelf (COTS) products are supported by this PWS. The Contractor shall comply with all applicable laws, policies, procedures, and apply federal Government best practices. The Contractor shall ensure all Cybersecurity and Information Technology projects, applications, systems, programs, or other areas of support provided hereunder comply with, adhere to and are guided by the standard program inception, elaboration, construction, and maintenance application life cycle.

This PWS supports both classified and unclassified programs on multiple external networks and security domains. Services requiring personnel with Secret and Top Secret clearances will be identified in the individual task orders written off of this IDIQ.

3.0 OBJECTIVES

The objective of this contract is to provide IT capabilities and services under an Indefinite-Delivery/Indefinite-Quantity (IDIQ) task order type contract. The Contractor shall have knowledge of business processes, the ability to analyze those processes in a holistic and integrated context, and recommend viable cost-effective technical and data solutions that improve operations and reduce costs. The Government's primary objectives under this contract are to secure an industry partner that:

- Provides flexible, scalable IT services that will enhance each supported activity's ability to respond to dynamic needs in their respective areas of responsibility.
- Delivers operational, technical and program efficiencies to drive down costs without compromising the timeliness or quality of services.
- Optimizes use of tools, technologies, bandwidth, capacity, and computing power in a manner that controls and reduces costs.
- Manages workload surges effectively and in a manner that, given mission requirements and competing priorities, efficiently schedules and applies resources to meet the needs of supported activities without one activity's needs being given primacy over the other.

The effort includes ensuring that systems are fully compatible and integrated with current software programs and functional in relation to existing operating environments to the greatest extent possible.

DMDC's portfolio is constantly evolving. It is anticipated that during the life of this order DMDC will augment and change tools to improve visualization, usability, speed of delivery of data and to create a more cost effective footprint. Lastly, the Contractor shall remain abreast of emerging technologies in the marketplace and recommend changes, modifications, upgrades, and industry best practices.

4.0 SCOPE

The scope of this contract is to provide IT services to support a common framework for the delivery of DMDC applications and systems supported under the EITS II contract. These IT services include the following components:

(a) **Enterprise services for DMDC systems and applications.** These enterprise services will ensure the consistent application of DMDC's service delivery model across DMDC's IT portfolio. Services to be provided under this requirement include enterprise architecture, enterprise application database management, and enterprise quality assurance.

(b) **Sustainment and Enhancement Services.** The scope of the sustainment and enhancement services spans the scope of the systems, applications, and databases that are identified in Appendix A.1 of this PWS.
As DMDC's portfolio changes, the list of systems and applications in Appendix A.1 will evolve during the life of the IDIQ to meet changing mission needs, based on the following:

1) As new programs and requirements are realigned to DMDC's portfolio, the Government will evaluate these capabilities to determine if the capability aligns with sustainment and enhancement requirements already supported within the EITS II portfolio. Requirements that are determined to align with current sustainment and enhancement work is within scope.
2) DMDC programs as they are modernized or realigned within the DoD or another federal agency will be removed from the EITS II portfolio. The Contractor will provide transition out services for these programs. Modernization under the EITS II IDIQ contract means major technical efforts, such as but not limited to:
    - re-platforming
    - re-hosting
    - recoding
    - re-architecting
    - re-engineering
    - interoperability
    - replacement and retirement

5.0 PERFORMANCE REQUIREMENTS

The Contractor shall provide support for the tasks described below:

5.1 TASK 1 – PROVIDE PROGRAM/PROJECT MANAGEMENT SUPPORT

Program Management includes the effective and efficient management of all contractor work including the accountability and security of all personnel. Program Management ensures that contractor performance is within agreed upon quality, cost, and schedule objectives and supports Government planning and decision processes with cost estimates, technical plans, status reports, performance estimates, and other decision support information. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this PWS.

The Integrated Master Plan (IMP) and Integrated Master Schedule (IMS) help establish and maintain that baseline and facilitate effective planning and forecasting that are critical to project success. The IMS includes distinct tasks that are summarized by risk and Work Breakdown Structure (WBS) identifiers so the program can track progress and measure schedule performance. The IMP and IMS should be traceable to the program, contractor WBS and the PWS.

In support of Task 1 - Program and Project Management subtasks, the Contractor shall:

5.1.1 Construct and manage an IMP and IMS including a WBS, critical path milestones, management approach, policies, procedures and suggested project metrics for each task order to provide a high-level picture of all project activities. The Contractor shall update, manage, and analyze proposed schedule changes providing the Program Managers with an assessment of impacts to the IMS in accordance with program, project or initiatives. The Contractor shall submit and maintain the IMP and IMS on the enterprise Microsoft Project server.

5.1.2 Provide information and recommendations to respond to Congressional, DOD, other Government agency, media or industry inquiries, Freedom of Information Act (FOIA) requests, audits and for Congressional testimony.

5.1.3 Maintain a real-time calendar of ongoing projects this includes maintaining, refining, and revising the project collaboration sites currently on SharePoint or other Government-designated repositories. This site must include project overview documents, a consistently updated document library that preserves document history, schedules, a dashboard, assignment and POC lists, summaries and agenda for all meetings and conferences attended, and support for collaborative editing/versioning of project documents.

5.1.4 Provide a Project Management Plan (PMP) that encompasses each awarded task order and that describes the proposed management approach, the milestones, tasks, and subtasks required by the individual task order. The PMP shall provide for an overall Work Breakdown Structure (WBS) and associated responsibilities. The Project Manager shall be responsible for a detailed PMP that identifies and assigns tasks, major milestones, dates and dependencies, and indications of critical path. The PMP shall include the status; statistics; risk management review; critical path; and other milestone progress checks and updates; as well as technical content review. The Government approved PMP will be used to monitor the Contractor's progress on the task orders. The PMP is an evolutionary document, any revisions are considered incorporated to any subsequent task order, upon written acceptance of the Government, inclusive of any changes to deliverables detailed in the PMP.

5.1.5 Coordinate with DMDC governance bodies such as DMDC Information Systems Security Group (DISSG), Developer's Steering Group (DSG), Enterprise Quality Assurance (QA), Configuration Management (CM), IT Operations, Customer Contact Center (CCC), DMDC Management Advisory Group (DMAG), production support, technical writing, implementation support, and other impacted divisions for project requirements and execution.

5.1.6 Identify, document, and execute risk planning and mitigation strategies that address exposure in the operation, maintenance, delivery, and deployment efforts of DMDC products. Identify and manage technical risk factors, including those related to execution of contract requirements.

5.1.7 Develop, maintain, enhance, and revise all required project documentation including project charters; concepts of operation (CONOPS); business requirements documents; integrated business use cases, user stories, and epics; functional designs and specifications; technical designs and specifications; requirements traceability matrices; process flow and activity diagrams; developer/technical use cases to support DMDC projects and programs; and end-user documentation.

5.1.8 Monitor legislative and policy changes; perform regulatory, legislative, policy and standards research and provide assessments to the government of impact to designated programs and IT products; and implement government directed legislative and policy changes.

5.2 TASK 2 – PROVIDE ENTERPRISE ARCHITECTURE (EA) SUPPORT

Enterprise Architecture is the transformational resource that translates business vision and strategy into effective enterprise change by creating, communicating, and refining the key insights (requirements, principles, models) that describe DMDC's future state and enable evolution and transformation. The goals of the Enterprise Architecture are to improve the organizational efficiency, effectiveness, and

agility by delivering business-aligned future states. Architecture shall comply with DoD and DMDC security policies and models.

5.2.1 Inform and advise DMDC leaders and staff on strategic and operational opportunities for improvement and develop roadmaps that illustrate feasible approaches to achieve them. Provide architectural insight for enterprise and IT-level strategy formation; providing models of future state, with roadmaps that steer the implementation of change initiatives.

5.2.2 Create an EA Vision and Plan that documents current and future state models and includes a roadmap of transitioning from current state to future state. Determine business drivers, constraints, architecture principles, initial architecture requirements, stakeholder concerns and EA deliverables and models to be produced to address these concerns.

5.2.3 Design and implement the architecture for various applications, including hardware, software, mainframe, and data for classified, un-classified, integration among applications, and cross-domain solutions. Identify tools and technologies that meet the new software development requirements as well as the DMDC current architectural approach.

5.2.4 **Business Architecture**

Application Architecture defines the framework of an organization's application solutions against business requirements. It looks globally within systems and designs business processes, selects the best software to support those processes and determines the development of dedicated solutions. It ensures the application landscape is scalable, reliable and complies with DoD and DMDC referenced architectures.

5.2.4.1 Conduct application architecture initiatives; identify and classify application components according to the specific business and performance objectives they support and the technologies employed.

5.2.4.2 Document and perform analyses of the current application inventory and provide detailed application architecture guidelines that improve both business and technology processes and applications.

5.2.4.3 Identify and recommend which applications should be delivered, what technologies should be used to deliver them, and how the applications should be designed, deployed and integrated in the most effective and flexible way. Identify regulations and legislation applicable to each inquiry.

5.2.4.4 Assess and document the alignment of applications and services to Agency programs.

5.2.4.5 Develop and maintain architectural design documents.

5.2.4.6 Identify problems, correctly attribute them to automated processes and/or submission data and develop solutions.

5.2.4.7 Respond to ad hoc research requests from DMDC management to include: performing special studies, conducting data research and respond to inquiries for DMDC internal customers, as well as external customers from within the DoD and the Federal Government.

5.2.5 **Infrastructure & Technology Support**

5.2.5.1 Conduct Enterprise requirements analyses, IT architecture and infrastructure planning, implementation, and maintenance.

5.2.5.2 Provide technology assessment evaluation on hardware and software, document hardware and software technology refresh recommendations.

5.2.5.3 Review and propose changes to charge-back methodologies.

5.2.5.4 Provide support in assessing performance of infrastructure in producing business value and return on investment.

5.2.6 **Enterprise Data Architecture (EDA)**

5.2.6.1 Coordinate enterprise efforts that affect data with a focus on data that moves through the enterprise.

5.2.6.2 Improve the consistency, timeliness, quality, security and delivery of data and streamline data flows eliminating unnecessary costs from the data architecture.

5.2.6.3 Define and document interfaces and movement of data through the enterprise.

5.2.6.4 Ensure data architecture meets performance, maintenance, and system requirements.

5.2.6.5 Create an enterprise-wide set of models, standards, glossaries and hierarchies which allow a standard description of data across business lines, products and functional areas.

5.2.7 **Integrated Solutions Management**

The requirements of this performance area include management and technical support for research, analysis recommendation and documentation of integration issues and approaches. The issues and approaches considered under this area evolve from a variety of sources such as external audits, technical reports, DOD and Federal standards, operational policies and doctrines, technical guidelines and best practices.

The Contractor shall assist the Government in performing the following activities for services required under this performance area:

5.2.8 **Business Process Reengineering (BPR)**

This performance area involves the use of Business Process Reengineering (BPR) as an approach for improving organization performance and covers the range of BPR activities including services needed to implement new or revised business and functional processes arising from BPR undertakings. The Contractor shall assist the government in examining organization goals, objectives, structures/hierarchies, cultures, systems and roles for the purpose of executing a ground-up redesign for achieving long-term, full-scale integration required by the agency. Improving performance and reengineering processes includes services in support of, and helping shape, the direction of DMDC security, including those applications and approaches to network defense required to protect from

unauthorized entry and intrusions, as well as measures designed to track and prevent future damage to DoD's communication capabilities.

5.2.9 **Cloud Implementation, Integration and Operations**

Provide support for integrating new applications and transitioning existing applications into virtualized/cloud environments. This support includes the entire cycle of transition events, from supporting the customer in acquiring cloud service provider enclaves, including market research and piloting efforts, to building out Virtual Data Centers and network architectures, installing applications and locking down environments, transferring any existing databases or other information from existing hosting solutions, supporting assessment and authorization of the new environments, and supporting testing activities in the virtualized environments. This effort also includes integration activities with Platform as a Service and Software as a Service offerings, as well as with other required services or systems (i.e., authentication services). This effort also includes development and implementation of strategies for data and application portability and storage to minimize vendor lock-in and data loss.

5.2.10 **Security Architecture**

5.2.10.1 Verify security systems. Maintain security by monitoring and ensuring compliance to standards, policies, and procedures; conducting incident response analyses; developing and conducting training programs.

5.2.10.2 Develop the architecture that incorporates systems security principles, Information Assurance controls and risk management concepts and best practices into organization-wide strategic planning considerations, core missions and business processes supporting organizational information systems.

5.2.10.3 Enhance security team accomplishments and competence by planning delivery of solutions; answering technical and procedural questions for less experienced team members; teaching improved processes; mentoring team members.

5.2.10.4 Determine security requirements by evaluating business strategies and requirements; researching information security standards; conducting system security and vulnerability analyses and risk assessments; studying architecture/platform; identifying integration issues; preparing cost estimates.

5.3 TASK 3 – PROVIDE ENTERPRISE DATABASE MANAGEMENT (DBM) SUPPORT

5.3.1 Create a Database Maintenance Plan that provides a set of critical specific tasks that need to be performed regularly to ensure adequate database performance and availability.

5.3.2 Define, build, orchestrate and manage database operating procedure run books that support operational processes.

5.3.3 Act as technical consultant to other database administrators; provide direction in planning, design, implementation, operations and management, installation, patching, tuning and configuration of database applications. Define processes and guide efforts for problem resolutions, troubleshoot, make recommendations and take action to ensure optimal performance of databases.

5.3.4 Produce entity relationship and data flow diagrams, database normalization schemas that are logical to physical data maps and data table parameters.

5.3.5 Create stored procedures, functions, views, triggers, constraints and analyze access patterns; proposing the best combination of indexes, constraints, foreign keys, and queries.

5.3.6 Respond to database service requests and contribute to plans and policies for the production management of critical, large and enterprise databases.

5.3.7 Design, implement, maintain, and repair databases for continuous operation. Specific database standards will be defined at the task order level. Generally, databases under this contract shall:

- reduce the time previously required to complete the same task by continuous operations with outages less than 5%.
- be executable in operation at all times unless they are being maintained or repaired.

5.3.8 Instruct application owners on new Relational Database Management System (RDBMS) features; provide analysis, performance impact, ease of use, and compatibility with existing environments.

5.3.9 Define project schema requirements and establish guidance on enterprise modeling standards as they apply to the production and test databases.

5.3.10 Conduct and identify logical database design and modeling, identify physical design requirements, tablespace and partitioning recommendations and collaborate with the data architects and the enterprise data modeler to review and publish application logical data models.

5.3.11 Maintain data integrity and availability for enterprise level databases, tables and structures.

5.3.12 Monitor and tune Structured Query Language (SQL) Data Manipulation Language (DML) statements stored in the database. Write database queries to extract information from the dynamic performance views and database administrator views in the database to identify problems. Collaborate execution of these queries with the systems database administration group and review results.

5.3.13 Monitor project storage consumption, identify storage usage trends and schedule database object reorganization. Coordinate with the application owners to identify project storage requirements and compute storage requirement.

5.3.14 Collaborate with the Configuration Management (CM) Team on deployments and processes.

5.3.15 Provide database restore and recovery in collaboration with IT Operations. Participate in the annual disaster recovery exercises and ‘point in time’ recoveries.

5.3.16 Perform database conversions, migrations and data extracts from production databases.

5.3.17 Support, maintain, and keep the test, development, and pre-production databases and database configurations consistent across environments and conduct database refresh of all database instances.

5.3.18 Verify the accuracy and completeness of the data in DMDC databases (e.g., Personnel Data Repository (PDR), Joint Verification System (JVS), Real-Time Automated Personnel Identification System (RAPIDS)/Common Access Card (CAC)).

5.3.19 Create and maintain a database maintenance dashboard that monitors resources, record application transaction volumes and tracks database volume.

5.3.20 Provide RDBMS network encryption requirements and identify encryption requirements for database connections. Monitor RDBMS log files and application log files for database related problems.

5.3.21 **Control Database Security**

5.3.21.1 Provide a database security plan that identifies all of the assets and data. Document responsible parties, locations, and unique identifiers for these assets providing an auditable record that may be referenced as needed for implementing security measures and investigating incidents.

5.3.21.2 Design data distributions and data archiving solutions with security measures in place to protect against computer threats.

5.3.21.3 Capture and monitor Data Dictionary Language (DDL) actions against test, model office, contractor test/prod sim and production databases. Report any unauthorized DDL activities to the government Information Assurance Officer.

5.3.21.4 Provide guidance to application owners on how to effectively query database tables. Review and suggest query improvements explaining the rationale behind the changes. Advise on RDBMS tools to assist in constructing efficient database queries.

5.3.21.5 Coordinate with developers and end-users on database usage, query development, tuning and to migrate objects and code between different environments.

5.3.21.6 Monitor for deviations implement appropriate policies and monitor any vulnerabilities that cannot be remediated for any and all activity the deviates from authorized activity.

5.3.21.7 Respond to suspicious behavior alert and respond to any abnormal or suspicious behavior in real time to minimize risk of attack.

5.4 TASK 4 – PERFORM SOFTWARE DEVELOPMENT LIFECYCLE (SDLC) SERVICES

Provide services for all phases of software design and development including deployment to ensure applications and databases enable users to meet mission goals and objectives **(Appendices D and E)**. These efforts include a wide range of software design, development, implementation and integration, and may include concept development, planning, requirements definition and analysis, systems design and development, coding and testing, production and systems support, deployment, implementation, integration, and software application maintenance.

Software development shall place emphasis on coding that is easily maintained, highly secure and compliant with DMDC coding practices. The Contractor shall maximize and facilitate code re-use by leveraging already existing or project specific software re-use libraries. Executable and source software

generated specifically for this task shall have all rights relinquished to the Government and, at the Government's discretion, be made available for other Government users to obtain.

5.4.1 **Requirements Gathering and Analysis**

5.4.1.1 Perform requirements gathering and analysis to include requirements analysis, feasibility, migration, business process reengineering, requirements validation through interaction with functional proponent, requirements traceability, business process modeling, rules, data requirements, and interface management. Document workflow, business processes, data and services, and include a standard set of artifacts for the purpose of understanding the program asset/software requirements.

5.4.1.2 Translate requirements to design modifications maintaining the integrity of the product's design.

5.4.1.3 Develop user scenarios, user interfaces, and provide oversight of development activities.

5.4.1.4 Provide business process-improvement support that includes all activities involved in helping improve customer data systems through business processes including rethinking program design and aligning information technology infrastructures with business missions, goals, and objectives.

5.4.1.5 Create data flow diagrams, perform data standardization and perform enterprise modeling, functional economic analysis, simulation/modeling, activity based costing and activity based management support.

5.4.1.6 Provide "as is "and "to-be" functional analysis.

5.4.2 **Design**

Perform design; describe system and software development and implementation processes. Document the requirements to be met by each element of the design and traceability to mission requirements. Document the software architectural design of each element and a description of each software unit.

5.4.2.1 **Software Development**

5.4.2.1.1 Support an agile and interactive development methodology (rapid development) and software development lifecycle with focus on the repetition of abbreviated work cycles and functional requirements. Software development shall be compliant with current DoD , DMDC and CMMI practices, processes and services.

5.4.2.1.2 Perform and document functional and technical requirements, create analysis and design documentation, program specifications, unit test criteria, code and test program units, and produce documentation.

5.4.2.1.3 Document code, conduct code reviews, include technical and functional specifications, applicable DODAF requirements and comply with DMDC configuration management requirements, including consistent application of effective version control. Deliver all software components including source code with release notes.

5.4.2.1.4 Provide Tier Level 3 support (24/7/365) for application outages in production and data issues escalated by the Customer Contact Center (CCC), program manager, or application helpdesk.

5.4.2.1.5 Update applications and infrastructure in support of DMDC infrastructure improvements, changes, technical refreshes, or migrations (e.g., CUF, AION migration, Data Center location transition). Assist the government in converting and testing software to run on new hardware or virtualization platforms.

5.4.2.1.6 Develop and execute Software Test Plan(s) to address application or system use cases, user interfaces, security considerations, and reports using test data designed to demonstrate compliance with all documented functional specifications for each release.

5.4.2.1.7 Perform planning, design, development, test and implementation of various static and dynamic content web sites; maintain and expand existing web pages.

5.4.2.1.8 Submit for review a testing report for each software package to the program manager after each software test; the testing report shall outline the result(s) of the software test plan for each item within the requirements traceability matrix.

5.4.2.2 **Software Maintenance and Sustainment**

Software Maintenance consists of correcting faults, improving performance or other attributes, adapting to a changing organization and technical environment and preventive maintenance. Software Sustainment involves orchestrating the processes, practices, technical resources, information and workforce competencies for systems and software engineering to enable systems to continue mission operations and be enhanced to meet evolving threat and capability needs. Provide all phases of software maintenance as defined in ISO/IEC 14764. The Contractor shall define, develop, trouble-shoot, and resolve problems during maintenance and sustainment. Maintenance shall include, correction, adaptive, perfective and preventive maintenance.

5.4.2.2.1 Create and maintain a Software Maintenance Plan of all maintenance actions. The plan shall indicate which maintenance tasks have been performed, when a particular maintenance task is not performed at its scheduled time and the reason and any future maintenance activities.

5.4.2.2.2 Develop and maintain a Software Quality Assurance Plan that details the subsystem and system level processes used to insure software products are tested and validated. Major events within the Software Quality Assurance Plan shall be reflected in the IMS. Implement a program to provide data quality assurance of software processes and deliverables.

5.4.2.2.3 Document code and version control releases. Deliver source and executable code and supporting documentation.

5.4.2.3 **Unit Testing**

5.4.2.3.1 Developers shall write unit tests to ensure that the unit (be it a method, class, or component) is working as expected and test across a range of valid and invalid inputs. In a continuous integration environment, unit tests shall run every time a change to the source code repository.

5.4.2.3.2 Conduct a verification of the interaction one or more new or modified coded product components, as well as dependent components that have not been modified, to ensure complete coverage of requirements and successful interaction of components prior to full system testing.

5.4.2.3.3 Conduct interface (system-to-system), stress and volume testing, as part of development testing to identify issues as early as possible, reducing the risk and cost of rework.

5.4.2.3.4 Create test data in all testing environments.

5.4.2.3.5 Version and maintain all test artifacts in order to perform repeatable and reliable testing.

5.4.2.3.6 Develop test plans, data and tools that exercise the application at both the unit and systems integration levels.

5.4.2.4 **Release Management**

Support the release cycle of each application to include installation, set-up, testing, and running of applications deployed within four (4) separate DMDC environments (see **Appendix B** for additional information on the environment configurations). Application deployment may require pre-loading of databases with a minimum set of valid test records, and provisioning a minimum number of users in each environment for access to the application(s). Comply with DMDC standards for common builds and apply configuration Management (CM) process specified in the Release Management Charter (see **Appendix E**) to all deployment items. This includes versioning application code for each deployment, building deployment packages, developing (and implementing, if required) back-out plans, recording and reporting the status of the deployed applications, and verifying the completeness and correctness of the deployed applications. Deployments will also require on-site and/or online training to personnel within the DoD community for using the deployed application.

5.4.2.4.1 Definitions for releases are as follows:

a. **Major Release** - Significant new capabilities and features, as well as large-scale defect fixes and occur infrequently. Major releases include significant code re-factoring and new development supporting a combination of major architecture, functional, or user interface level changes within the release.
b. **Minor Release -** Limited set of new features and functionality, tend to be more feature-laden than bug-fix-laden. Minor releases include limited architectural, functional, or user interface level changes within the release. Bug fixes and security patches could also be included.
c. **Maintenance Release** - Addresses defects or enhancements.

5.4.2.4.2 Manage system software, hardware, and configurations, to include patches, emergency data fixes, and upgrades for each release. Inform system users of upcoming releases that will change or increase system functionality or capability.

5.4.2.4.3 Ensure each release is compliant with Risk Management Framework requirements to gain certification as required by DoD Information Assurance and DMDC policies. Ensure monthly IAVA issues are monitored and resolved. Coordinate new releases with stakeholders, hosting facility and owners of connected systems. Coordinate with and allow system access to the Government IA representative for routine testing and data collection as necessary or requested to comply with IA requirements to obtain or retain Authority to Operate.

5.4.2.4.4 **Application Level Change Management**

Manage and maintain the existing automated software build and deployment infrastructure for each deployed application in support of the following environments: stand-alone workstations, LAN/WAN

development, LAN/WAN Test, and LAN/WAN Quality Assurance (QA). This includes but is not limited to overseeing the source code repository, infrastructure, common library components, and scripts required to perform CM automation. Coordinate with DMDC Release Planning to monitor, coordinate and stage required artifacts for each scheduled release. Software will be staged based on scheduled and out of-cycle release planning in support of the following environments. The environments may include the following: stand-alone workstations, LAN/WAN networks, Contractor Test, Stress Test and Production. Government review and approval is required prior to promoting to production environments. Provide a pre-deployment checklist to ensure all software is accounted for in each release and process change requests managed through the DMDC Configuration Management infrastructure.

5.4.2.5 **Configuration Management (CM)**

5.4.2.5.1 Manage the baseline configuration of the platforms, systems, subsystems and apply Configuration Management (CM) techniques that establish and maintain the integrity of the system. Provide configuration control support that includes analysis, change recommendations, tracking and reporting. Identify and document the characteristics of a configuration item, to control changes to a configuration item, and to record and report change processing and implementation status. (See **Appendices G.1 and G.2**).

5.4.2.5.2 Develop and maintain Configuration Management Plan (CMP). The Contractor's methodology must provide CM support for both program and engineering management functions, and apply configuration identification to all program elements whose physical and functional properties need to be managed and directly controlled

5.4.2.5.3 Collect, review, track and archive Configuration Control Documents and deliver all software components with release notes.

5.4.2.5.4 Support functional requirements traceability and the establishment of configuration items and configuration baselines, including functional baselines and product baselines.

5.4.2.6 **Production Support**

5.4.2.6.1 Monitor process and software changes that impact production support, communicate project information to the production support staff and raise production support issues to the product owner. Support scheduled and unscheduled, on-request and end-user initiated processing of business applications.

5.4.2.6.2 Maintain a run log for all batch applications. Implement procedures for proactively identifying, preventing, and responding to problems. Provide ongoing running and monitoring of batch systems, such as the personnel data feeds, Security, Point in Time and Database Extract.

5.4.2.6.3 Maintain and support all Test, Model Office, user acceptance test, benchmark test, stress test, and Production regions, including systems and applications components Support updates and monthly loads of address validation software.

5.4.2.6.4 Develop and maintain Disaster Recovery Activity (DRA) and COOP plans for every required application and interface.

5.4.2.6.5 Provide escalation support to understand, troubleshoot, root cause, log analysis and resolve complex technical issues.

5.4.2.6.6 Provide daily support with resolution of escalated tickets and act as liaison to product and technical leads to ensure issues are resolved in timely manner. Communicate with source of escalation, complete appropriate documentation, and process tickets according to agency methodology.

5.4.2.7 **Requirements Traceability Matrix (RTM)**

Create or update a Requirements Traceability Matrix for all projects. The RTM shall clearly link the new and/or changed requirements to where and how they have been implemented in the system. The RTM shall provide backwards and forward traceability, meaning the RTM documents each requirement from its source through definition, analysis, design, testing, acceptance, and deployment.

5.4.2.8 **Cyber Security/Information Assurance (IA) Support**

5.4.2.8.1 Ensure that all system or application deliverables meet the requirements of DoD and DMDC Information Assurance (IA) policy and that personnel performing IA activities obtain, and remain current with, required technical and/or management certifications. Protect system information and resources according to established security policies and procedures and ensure application code is updated with the latest security patches to minimize security vulnerabilities.

5.4.2.8.2 Provide documentation and confirm that application code changes comply with the DoD system security policy and are properly certified and accredited in accordance with DODI 8510.01 Risk Management Framework (RMF). Provide engineering, cyber security and IA services consistent with established disciplines and best practices for effective systems engineering, systems security engineering, and program protection planning outlined in DoDI 5000.02.

5.4.2.8.3 Provide documentation to support RMF Certification and Accreditation processes. Final approval for all IA tasks under this contract belongs to the Information Assurance Officer, Cybersecurity Branch. The Contractor shall obtain final approval from Cybersecurity. All IA-related design decisions, including cryptography, authentication, access control, data transfer and storage, Need-to-Know (NTK), or other IA technologies, must be coordinated with and approved by the cognizant representative of the Cybersecurity Branch.

5.4.2.8.4 Identify potential program, system, and engineering risks that pertain to cybersecurity; and participate in and support the development of risk mitigation plans and monitoring of risk mitigation activities.

5.4.2.9 **Technical Writing**

Prepare required end user and technical documentation, online help, reference materials, standard operating procedures and release notes. Tasks shall include but not be limited to:

a. maintain configuration management control of all documents
b. develop and maintain documentation related to the hardware, software application, and/or on-line (web site) sources of data;
c. maintain the DMDC documentation library
d. develop and maintain user documentation and on-line help
e. develop training materials and documentation
f. develop documentation of systems, applications, and processes

g. Ensure all documents are properly checked into SharePoint with the proper meta-data and tags allowing easy retrieval of required documents and information

5.4.2.10 **Software and Systems Integration/Implementation**

5.4.2.10.1 Facilitate and monitor the integration, interoperability, and synchronization of enterprise-wide systems and infrastructure solutions and services.

5.4.2.10.2 Develop a systems integration plan to oversee the development of external dependent projects and provide a strategy for the successful integration of all software and hardware into the environment. Plan to include roles and responsibilities, assumptions, internal and external stakeholders, integration/coordination with external organizations, implementation schedules and status, interdependencies of applications, systems integration, design review and acceptance procedures and schedules, user acceptance testing support, privacy and security management (site security, data privacy/security), and defect tracking and resolution.

5.4.2.11 **Software Transition Support**

The Contractor shall provide support for transition of the delivered software/software components to the Government or Government-specified Contractor, to include, but not be limited to, performing software test and verification, training, and corresponding documents that provide information on the use and maintenance of the software and its components. The Contractor shall prepare a project specific Software Transition Plan. The Software Transition Plan shall address products to be turned over (documentation, software, hardware, tools), formats and media, schedules, and support during transition. The Contractor shall include all resources needed to control, copy, and distribute the software and its documentation. The Contractor shall identify at the Test Readiness Review all hardware and software that will be transitioned during each delivery and the time frame of the transition.

5.5 TASK 5 – CONDUCT ENTERPRISE QUALITY ASSURANCE (QA) TESTING

This task ensures that systems, applications and software delivered by the development teams are functional, stable, and secured. Testing personnel shall not be involved in any stage of the software requirements, design or development process. The purpose of the testing is:

a. Verification Check whether the product meets the stated requirements, specifications or constraints
b. Validation Determine whether the product achieves its intended purpose and meets the needs of the stakeholder

5.5.1 Conduct enterprise-wide testing to include but not limited to: online and batch processing, thick-client, web applications, web services, operator based and self-service portlets, system to system interfaces, database objects, shared library components, and integration to third party products and external organizations and other related software components.

5.5.2 Define and develop test plans, test scripts, test cases; track and report issues; conduct testing and measure the success during and after testing; and evaluate and document test results. Types of testing includes, but is not limited to:

a. Functional
b. Integration
c. Performance
d. Regression

e. Compliance
f. System/ end-to-end
g. User Acceptance
h. Usability
i. 508 Compliance
j. Stress
k. Load
l. Boundary
m. Exploratory

5.5.3 Produce consistent, cost-effective results that consider security at every phase, identify issues and facilitate speedy implementation of measures to avoid or mitigate risks.

5.5.4 Provide a perspective on tests and results and allow assessment of the technical and operational impact of any identified noncompliance.

5.5.5 Identify, analyze, and document software defects; assist developers in analyzing and resolving defects. Review quality control processes and identify areas needing improvement.

5.5.6 Maintain, test and support QA testing tools.

5.5.7 Conduct Quality Assurance (QA) using documented requirements provided in functional, technical or application release scope specifications.

5.6 TASK 6 - OPERATE THE COMMON ACCESS CARD (CAC) CENTRAL ISSUANCE FACILITY (CIF)

The CIF is the Department of Defense's (DoD) enterprise solution for bulk production and issuance of CAC cards and their PINs for more than 200,000 new recruits and other DoD personnel annually by collecting required demographic and identity information, processing that data to produce the cards centrally, and shipping the cards to pre-determined locations including eight basic training sites, three academy sites, and two officer training schools.

5.7 TASK 7 - SURGE SUPPORT

Surge will be identified in individual task order if required. As an agency of the DoD, DMDC must respond to real-world changes, whether it is a new reform initiative, top-down policies and mandates, or even national security interests and immediate threats. It is essential that DMDC have the IT resources and means to support evolving threats. Projects include, short-term (less than 90 calendar days) response to implement directives, support to cybersecurity-related events, and surge to support complex upgrades. The Contractor shall provide staffing resources within scope of the current contract to fulfill unplanned projects or unanticipated requirements. The Contractor shall use industry best practices and subject matter expertise to execute additional, as needed, related projects.

Surge support shall include, but is not limited to, the following activities:

a. Additional resources to support the relocation of DMDC applications/systems
b. Rapid capabilities that mitigate or resolve major IT issues, cybersecurity threats, national security events, policy changes, and impacts
c. Implementation of new DoD programs
d. Transition or transfer of existing DoD programs

The Contractor shall account for additional as-needed activities and provide the resources necessary to accommodate them. During the life of this contract the workload in any one area may grow significantly for a period of time. When a surge requirement is identified by the Government, the surge CLIN will be exercised and the surge requirements will be provided to the Contractor in a document specifying the surge requirements, schedule, and expected outcomes. The Contractor shall develop a Surge Plan which shall include, project approach, milestones and schedules, and detailed resource information to be reviewed and approved by the Government. Unless specified differently at the task order level, the Contractor shall staff surge resources within 30 calendar days of formal written approval of the Surge Plan.

5.8 TASK 8 - PROVIDE INTELLIGENCE AND INVESTIGATION SUPPORT

5.8.1 Provide administrative and logistical support for cyber field operations, supporting the DoD goal of strengthening cyber capabilities and expertise to ensure reliability of applications and systems while countering and preventing threats in a fast-paced, responsive and accurate manner.

5.8.2 Provide functional and technical expertise concerning Cyber operations including: planning, execution, analysis and performance of decision processes, applications and systems such as architecture, vulnerability, methodologies, operations monitoring and data structures.

5.8.3 Provide support to select intelligence and special operations organizations for myriad historical and future requirements and other unclassified and classified activities and initiatives across all intelligence disciplines.

5.8.4 Provide support to Human Intelligence (HUMINT), Counterintelligence, and Counter-Terrorism activities and support these missions to enhance personnel /force protection, OPSEC, modernization and training.

5.8.5 Provide business analytical support to DoD and other Federal organizations as well as within the intelligence, federal law enforcement and special operations communities.

5.8.6 Provide risk assessments for internal DMDC management in order to assist in the identification of adversarial information, technical applications and specific information technologies.

5.9 TASK 9 – PLANS, REPORTS, AND DOCUMENTATION

5.9.1 **Technical Roadmap**

Provide a Technical Roadmap that is updated annually which makes recommendations for DMDC consideration to drive innovation, process improvement, efficiencies, and leverages emerging technology. Incorporate lessons learned from the prior year in each annual update. Provide a proposed schedule and milestones for technology recommendations and a recommended approach to reduce Total Cost of Ownership across DMDC's portfolio.

5.9.2 **Communications Plan**

Develop and deliver a Communications Plan that provides methods, timing, roles, responsibilities and key messages. The Communication Plan shall describe how the Contractor will establish a reliable means of communicating status about the contract to all appropriate stakeholders. It describes what needs and

how it will be communicated, who is responsible for communicating with whom and when the communication needs to take place.

5.9.3 **Risk Management Plan**

The Contractor shall develop a Risk Management Plan that shall address cost, schedule, technical, project, and program risks. The technical risks shall include design, requirement volatility, security, operations, and technology factors. The Contractor shall submit a Risk Management Plan to the COR and shall update the plan at least annually.

5.9.3.1 Document risks in a risk management system and review weekly with Service Delivery Product Owners at a Risk Review Board, with representation from key project areas.

5.9.3.2 Assist in the identification of risks associated with the technologies included in program/project solutions and risks associated with the methods and techniques used to develop those solutions.

5.9.4 **Meeting Summaries**

The Contractor shall participate in telephone conferences and meetings to discuss on-going technical performance and problems. These calls are used to summarize activities that have been performed since the previous call and discuss the status of activities going forward. The Contractor shall attend additional meetings as specified by the Government and provide meeting summaries. Participate and contribute to various agencies technical meetings to include Technical Working groups and various ad hoc technical tiger teams.

5.9.5 **Weekly In-Progress Review (IPR)**

Conduct a Weekly In-Progress Review (IPR) to discuss program, project and service status, existing or potential problems, and projected tasks and milestones. The Contractor shall provide updates for activities in the PMP at the IPR. The Contractor shall participate, document, and distribute minutes of regularly scheduled weekly status report meetings. The Contractor shall meet with the Government Program Manager(s) to discuss technical matters, share ideas, review milestones, discuss activities accomplished, discuss new and current issues and work progress, as well as discuss and resolve outstanding administrative or managerial issues.

5.9.6 **Monthly Status Report (MSR) and Senior Management Reviews (SMR)**

The Contractor shall:

5.9.6.1 Deliver, in format approved by the COR, a Monthly Status Report (MSR) slide deck at least 3 business days prior to the scheduled SMR presentation.. The slides will be presented during Senior Management Reviews to report on the status and progress of the Contractor's previous month's performance of each task order. The final, Government approved, MSR shall be uploaded to the GSA ASSIST portal within two business days following completion.

5.9.6.2 The Contractor shall schedule and conduct a Senior Management Review (SMR) briefing by the 20th business day of each month covering the activities occurring in the prior month (e.g. presentation on February will cover Jan 1-31).

5.9.6.3 Conduct Senior Management Review meetings each month to brief Government stakeholders on the status of the work being performed under the EITS II contract. In support of each meeting, the Contract shall prepare an agenda and meeting minutes in a clear, concise and orderly manner. Briefing materials shall be made available to all attendees not less than 3 calendar days prior to time of briefing. The Contractor's Program Manager shall be on site for monthly SMRs, unless forbearance is authorized by the GSA or DMDC COR.

5.9.6.4 The SMR should include data of sufficient detail to monitor the completion of work products against progress as documented in the PWS. Topics to address include but are not limited to:

- Task Order Summary
- Summary of accomplishments for each project
- Deliverables delivered, status of deliverable comments
- Performance Metrics
- Significant Open Issues, Risk, Impact and Mitigation Action
- Summary of Open Problem Notification Reports (PNRs)
- Summary of Open Contractor Discrepancy Reports (CDRs)
- Summary of Issues Closed, in the reporting period, including CDRs and PNRs
- Status of corrective actions
- Integrated Master Schedule
- Milestones achieved or missed
- Burn Rate and funding status by task order
- Number of personnel on contract
- Subcontractor Identification Performance discuss 1st Tier subcontractors and vendor performance
- Task deliverables timeliness against plan
- Projected Activities for Next Reporting Period
- Upcoming events

The Government reserves the right to modify status reporting requirements at its discretion. The Contractor shall comply with any revised status reporting requirements at no additional cost to the Government.

5.9.7 **Problem Notification Report (PNR)**

The Contractor shall implement and maintain a Problem Notification Reporting system that provides timely notification to government representatives at DMDC and GSA who have responsibility for administering and managing the IDIQ and its task orders.

The Contractor shall provide immediate verbal notification to the DMDC COR when encountering a problem or risk event that significantly impacts the cost, schedule, or performance of the Order (or any deliverable or project under a task order). The Contractor shall provide a written PNR to the DMDC COR and GSA CO/COR not more than three business days after the identification of the problem.

All PNRs must be tracked in the SMR and through in-progress reviews (IPRs) until the Government agrees they are resolved. In the SMR, provide a summary of all open PNRs, as well as PNRs closed during the reporting period.

The PNR shall include, but not be limited to, the nature and sources of the problem and details addressing all data elements identified within the PNR Template provided under **Appendix R**, inclusive of any actual or potential impact on cost, delivery schedule, or deliverables affected; the extent of a delay (if any); steps to be taken to bring performance back on schedule; and corrective action needed to resolve the problems; action required by the Government; and the extent of any anticipated increase on cost (if any) to the Government.

5.9.8 **Contract Discrepancy Report (CDR)**

In the event of unsatisfactory contractor performance, the COR or CO will issue a CDR that will explain the circumstances and findings concerning the incomplete or unsatisfactory service. The Contractor shall acknowledge receipt of the CDR and respond in writing as to how he/she shall correct the unacceptable performance and avoid a recurrence. The Government will review the Contractor's corrective action response to determine acceptability and will use any completed CDR as part of an overall evaluation of Contractor performance when determining present or future contractual actions.

5.9.9 **Semi-Annual Subcontract Reporting**

The Contractor shall provide Ability-One and Subcontractor reporting data under the contract, segregated for each task order on a semi-annual basis within 15 calendar days beginning at the start of each Option Year. This data shall include:

- the name of the subcontractor(s),
- the overall percentage of the work (by hours and dollars) supported by the prime and each of the subcontractor(s).
- support provided by Americans with Disabilities (number of FTE and percentage) by task order.

	Name of Prime	**Name of Subcontractor 1**	**Name of Subcontractor 1**	**Number of full-time Americans with Disabilities Supporting each order**	**Percentage of work supported by Americans with Disabilities on each order**
Task Order 1	% hours by prime	% hours by sub	% hours by sub		
	% dollars by prime	% dollars by sub	% dollars by sub		
Task Order 2	% hours by prime	% hours by sub	% hours by sub		
	% dollars by prime	% dollars by sub	% dollars by sub		
…	…	…	…	…	…
Aggregate Total					

5.9.10 **Transition Plan**
The Contractor shall support any future transitions and integration efforts and provide a plan for transition services to ensure minimum disruption to vital Government business. This plan shall address how the Contractor shall work with the incumbent and Government personnel to ensure that there will be no service degradation during and after the transition-in period (initial ninety (90) calendar day period after date of contract and/or task order award) and during the transition-out period (ninety (90) calendar day period prior to date of contract and/or task order expiration). Prior to the end of the period of performance the Contractor shall begin to transition all data, information, training material, all deliverables, etc., to the office (either Government or Contractor) to perform the tasks in the PWS

5.9.11 **Transition-Out Plan**
If programs are transitioning out, the transition-out plan shall be delivered 30 calendar days after GSA notified the contractor of a specific transtion out activity. The Contract shall submit a Contract Transition-Out plan 90 calendar days prior to end of period of performance of the contract.

5.10 Quality Management System
The Contractor shall establish a quality management system that ensures compliance with applicable federal mandates, terms and conditions of the contract, performance standards, and industry best practices. Consider as part of its Quality Control Plan (QCP) a number of standard approaches toward quality such as the International Standards Organization (ISO) and Systems Engineering Institute/Capability Maturity Model (SEI/CMM) processes. Specific quality requirements may be provided at the individual task order level.

5.10.1 **Quality Control Plan (QCP)**
The Contractor shall maintain a written QCP that shall reflect the Contractor's overall approach, internal management controls and processes for delivery services that meet required performance standards and its procedures for reporting to the Government on identified aspects of quality issues. The QCP shall identify the means by which the Contractor will ensure quality effectiveness and demonstrate comprehensive management and review of data. The QCP shall describe what is measured, how often it is tracked and provided, who reviews and assures that appropriate action is initiated when trends are unfavorable, who the Government will contact for contractor quality issues, what method and process is used to track and resolve issues, where reports are sent and maintained, and how often quality issues are reviewed and reported. The QCP shall identify how the Contractor identifies and resolves deficiencies, identifies potential improvements, and maintains and makes available to the Government, documentation reflecting quality control inspections and any corrective actions taken. The Contractor shall provide copies of all discrepancies to the COR.

The Contractor's program for Quality Control shall assure that work complies with the requirements of the contract. The QCP will be reviewed for compliance by the Product Owner and COR. The Contractor shall make appropriate corrections and modifications to the plan and obtain acceptance of the plan before the start of the first operational performance period. Updates shall be provided whenever there is a change.

Develop and maintain an inspection system that encompasses all requirements of the task order. The inspection system shall satisfy the requirements within this PWS and shall be designed to keep the Contractor's management informed of all issues affecting quality.

Develop the QCP based on accepted industry standards and detail the processes, procedures, and metrics for assuring quality. The QCP shall also include establishment of capable processes; monitoring and control of critical processes and product variation; establishment of mechanisms for feedback of field performance and implementation of an effective root cause analysis and corrective action system.

5.11 Quality Assurance

The Contractor shall implement Quality Assurance program to increase performance and reduce the risk of projects, operations and associate contractor failure. The program shall emphasize deficiency detection, prevention and address timely corrective actions for unsatisfactory performance.

5.11.1 Prepare a Quality Assurance Plan that describes the Contractor's Quality Assurance Program and submit the original plan and any changes to the COR for approval prior to implementation. The Plan shall describe the Contractor's methods to monitor projects and ensure all PWS requirements are completed in accordance with specifications and industry standards

5.11.2 The Quality Assurance Plan shall include contractor conducted customer surveys. The Contractor shall conduct these surveys to determine customer satisfaction with the infrastructure operations, maintenance services, and provide the results of the surveys to the COR.

5.11.3 The Quality Assurance plan shall include a customer comments and complaint program. The program shall allow identification and correction of validated customer complaints, and provide feedback to the Government and customers on corrective action(s) taken. The term customer refers to customers internal and external to the organizations identified by this individual task orders.

6.0 DELIVERABLES

The Contractor shall submit a draft version of each deliverable and the government will provide written acceptance, comments and/or change requests, if any, in accordance with PWS Section 7.0. The Contractor shall make any corrections and submit the final deliverable, in accordance with the dates listed in the following table and in accordance with PWS Section 7.0:

Note: Individual task orders may have additional deliverables that will be defined within each task order PWS.

PWS Section	Deliverables	Date Due/Frequency
5.1	PMP, inclusive of: • Integrated Master Plan (IMP) • Integrated Master Schedule (IMS)	• Draft due within 30 calendar days of contract award • Final due iaw Inspection and Acceptance clause • Updated monthly
5.2.2	Enterprise Architecture Vision and Program Structure Plan	• Draft due within 60 calendar days of contract award and 30 calendar days after each option year is exercised
5.9.1	Technical Roadmap	Due November 15, 2019 and 45 calendar days after each option year is exercised
5.9.2	Communication Plan	• Draft due 10 calendar days after contract award. • Final due iaw Inspection and Acceptance clause • Updated as needed

5.9.3	Risk Management Plan	• Draft due 30 calendar days after contract award. • Final due iaw Inspection and Acceptance clause • Updated as needed
5.9.4	Meeting Summaries	3 business days after the meeting.
5.9.5	Weekly In-Progress Review (IPR)	Written report is due 1 business day prior to meeting; the day of the week the meeting will be scheduled will be determined per task order
5.9.6	Monthly Status Report (MSR) and Senior Management Reviews (SMR)	Monthly, by the 20th of each month; Electronic copy of brief shall be delivered 3 business days prior to the brief.
5.9.7	Problem Notification Report (PNR)	3 business days after identification of problem
5.9.8	Contract Discrepancy Report (CDR)	Respond to CDR in accordance with the requests from GSA Contracting Officer
5.9.9	Semi-Annual Subcontract Reporting	The report shall be submitted within 15 calendar days after each 180 calendar days of performance beginning at the exercise of each option.
5.9.10	Transition Plan	Transition-In Plan-90 calendar Days after Contract and/or Task Order award If programs are transitioning out, the transition-out plan shall be delivered 90 calendar days prior to end of period of performance of the Contract and or Task Order .
5.10.1	Quality Control Plan (QCP)	• Draft due 15 calendar days after contract award. • Final due iaw Inspection and Acceptance clause • Updated as needed
5.11.1	Quality Assurance Plan	• Draft due 15 calendar days after contract award. • Final due iaw Inspection and Acceptance clause • Updated as needed
8.4	Breach Report	1 business day after the breach
8.5	Organizational Conflict of Interest	The contractor shall immediately notify the Government of any potential OCIs and provide mitigation strategies.
8.8	Non-Disclosure Agreement	Prior to any contractor personnel reporting for work on individual task orders
10.1	Post Award Conference	NLT 5 business days after contract award
10.5.1	Tele-work Report	Annually
10.7.2	Trip Reports	5 business days after the trip unless forbearance is granted by the Government
11.2	Staffing Roster	Monthly

7.0 INSPECTION AND ACCEPTANCE

Inspection of all work performance, reports, and other deliverables under this Contract shall be performed by the Technical Points of Contact (TPOCs) designated post award. Acceptance of all work performance, reports, and other deliverables under this Contract shall be performed by the COR designated post award.

Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the government have been corrected. The general quality measures, set forth below, will be applied to each deliverable:

- Accuracy deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand, legible, and relevant to the supporting narrative. All acronyms shall be clearly and fully specified upon first use.
- Specifications validity all deliverables must satisfy the requirements of the government.
- File editing where directed, all text and diagrammatic files shall be editable by the government.
- Format deliverables shall follow dmdc guidance. Where none exists, the contractor shall coordinate approval of format with the COR.
- Timeliness deliverables shall be submitted on or before the due date specified.

7.1 DRAFT DELIVERABLES

The Government will provide written acceptance, comments and/or change requests, if any, within ten (10) business days from Government receipt of a deliverable.
Upon receipt of the Government comments, the Contractor shall have ten (10) business days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

7.2 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The Government shall provide written notification of acceptance or rejection of all final deliverables within ten (10) business days (unless specified otherwise). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

7.3 SCOPE OF INSPECTION

Deliverables will be inspected for content, completeness, accuracy and conformance to requirements. Inspection may include validation of information or software through the use of automated tools, testing or inspections of the deliverables, as specified in the specific task order(s). The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality and adequacy of deliverables.

The Government requires a period not to exceed fifteen (15) business days after receipt of final deliverable items for inspection and acceptance or rejection.

7.4 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the task order(s), the Contractor's proposal and other terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

For software development, the final acceptance of the software program will occur when all discrepancies, errors or other deficiencies identified in writing by the Government have been resolved, either through documentation updates, program correction or other mutually agreeable methods Reports, documents and narrative type deliverables will be accepted when all discrepancies, errors or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments to deliverables must either be incorporated in the succeeding version of the deliverable or the Contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains excessive spelling errors, grammatical errors, improper format, or otherwise does not conform to the requirements stated within this Contract and subsequent Task Orders, the document may be immediately rejected without further review and returned to the Contractor for correction and resubmission. If the Contractor requires additional Government guidance to produce an acceptable draft, the Contractor shall arrange a meeting with the TPOC/COR.

7.5 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the Contractor, within ten (10) business days of the rejection notice. If the deficiencies cannot be corrected within ten (10) business days, the Contractor will immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within ten (10) business days.

8.0 RECORDS/DATA

The Government will be sole owner of all technical data, software developed, and infrastructure designed under this project. The Contractor shall deliver to DMDC all software, software licenses, data, form, fit and data first produced (including source code), written documents and reports to include, at a minimum, system change plans, various operations procedures and planning documents, meeting minutes, reports, manuals, training text, program management reviews, financial status reports, and any other documents created in support of this agreement or task orders. All system documentation shall be updated to remain current with each software development activity/phase. The Government will include the actual requirements, formats, delivery schedules and points of contact in each order. DMDC will have unlimited rights as allocated under FAR 52.227-14(b) in all data delivered under the orders. Unless otherwise stated in the orders, the Contractor shall submit deliverables to the COR or his or her designee. The Government will include review times and response to review comments in the orders. The COR will serve as DMDC's focal point for accepting the deliverables unless an order provides for other procedures.

8.1 DATA RIGHTS

The Government requires unlimited rights in any material first produced in the performance of this contract or any task order, in accordance with the FAR clause at 52.217-14. In addition, for any material first produced in the performance of a task order, the materials may be shared with other agencies or contractors during the period of performance of the task order, or after its termination. For any subcontractors or teaming partners, the Contractor shall ensure at proposal submission that the

subcontractors and /or teaming partners are willing to provide the data rights required under the task order.

8.2 LIMITED USE OF DATA

Performance of this effort may require the Contractor to access and use data and information proprietary to a Government agency or Government Contractor which is of such a nature that its dissemination or use, other than in performance of this effort, would be adverse to the interests of the Government and/or others. Contractor and/or Contractor personnel shall not divulge or release data or information developed or obtained in performance of this effort, until made public by the Government, except to authorize Government personnel or upon written approval of the Contracting Officer (CO). The Contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as required in the performance of this effort. Nothing herein shall preclude the use of any data independently acquired by the Contractor without such limitations or prohibit an agreement at no cost to the Government between the Contractor and the data owner which provides for greater rights to the Contractor.

8.3 DISCLOSURE OF INFORMATION

Information made available to the Contractor by the Government for the performance or administration of this effort shall be used only for those purposes and shall not be used in any other way without the written agreement of the Contracting Officer. The Contractor agrees to assume responsibility for protecting the confidentiality of Government records, which are not public information. Each Contractor or employee of the Contractor to whom information may be made available or disclosed shall be notified in writing by the Contractor that such information may be disclosed only for a purpose and to the extent authorized herein.

8.4 BREACH RESPONSE

DoD 5400.11-R, "DoD Privacy Program," May 14, 2007, defines a breach as the "actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected." The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data. The Contractor shall also ensure the confidentiality, integrity, and availability of Government data in compliance with all applicable laws and regulations, including data breach reporting and response requirements, in accordance with DFAR Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoDD 5400.11, "DoD Privacy Program," May 8, 2007, and DoD 5400.11-R, "DoD Privacy Program," May 14, 2007. The Contractor shall also comply with federal laws relating to freedom of information and records management. Upon discovery of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access, the contractor/subcontractor shall immediately and simultaneously notify the COR, the designated Cyber Security Officer, and Privacy Officer for the contract within one (1) hour. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to DMDC assets, or sensitive information, or an action that breaches DMDC security procedures.

The Contractor shall adhere to the reporting and response requirements set forth in the Office of the Secretary of Defense (OSD) Memorandum 1504-07, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," June 5, 2009; DoD 5400.11-R, and applicable DMDC Privacy Office guidance. The Contractor shall, at their own expense, take action to mitigate, to the

extent practicable, any harmful effect that is known to the Contractor of a use or disclosure of Protected Information by the Contractor in violation of the requirements of this Clause.
In the event of a data breach or privacy incident involving contractor processes under this contract, the Contractor shall be liable to DMDC for liquidated damages for a specified amount per affected individual to cover the cost of providing credit protection services to those individuals.

8.5 ORGANIZATIONAL CONFLICT OF INTEREST

Contractor and subcontractor personnel performing work under this contract may receive, have access to, or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.), or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

8.6 NON-DISCLOSURE REQUIREMENTS

All contractor personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the contract issued which requires the contractor to act on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, shall execute and submit a Contractor Non-Disclosure Agreement" Form. This is required prior to the commencement of any work on such task order and whenever replacement personnel are proposed under an ongoing task order. Any information obtained or provided in the performance of this contract is only to be used in the performance of the task order. The Contractor shall take the necessary steps in accordance with Government regulations to prevent disclosure of such information to any party outside the Government and to indoctrinate its personnel who have access to sensitive information and the relationship under which the Contractor has possession of or access to the information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information will be used for the profit of any party other than those furnishing the information. The Nondisclosure Agreement for Contractor Employees shall be signed by all indoctrinated personnel and forwarded to the Contracting Officer Representative (COR) for retention, prior to work commencing. The Contractor shall restrict access to sensitive/ proprietary information to the minimum number of employees necessary for contract/Task order performance.

8.7 CONTRACTOR TRAINING REQUIREMENTS (5 CFR 930.301(1))

If contractors/subcontractors use Government computers, they shall complete DMDC sponsored IT Security Awareness training. Other DMDC mandated training courses include:

- Records Management
- Insider Threat
- Environmental Management System (West cost only)
- Information assurance (IA)/Cyber Awareness Challenge Training
- Privacy act and Personally Identifiable Information (PII) (combined) - Civil Liberties
- Counter Intelligence (CI) Awareness

8.8 SECTION 508 COMPLIANCE

Unless the Government invokes an exemption, all EIT products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 CFR 1194. The Contractor shall identify all EIT products and services proposed, identify the technical standards applicable to all products and services proposed and state the degree of compliance with the applicable standards. Additionally, the Contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The Contractor must ensure that the list is easily accessible by typical users beginning at time of award.

The Contractor must ensure that all EIT products and services proposed that are less than fully compliant, are offered pursuant to extensive market research, which ensures that they are the most compliant products available to satisfy the solicitation's requirements.

If any such EIT product or service proposed is not fully compliant with all of the standards, the Contractor shall specify each specific standard that is not met; provide a detailed description as to how the EIT product or service does not comply with the identified standard(s); and shall also indicate the degree of compliance.

8.9 ENTERPRISE-WIDE CONTRACTOR MANPOWER REPORTING APPLICATION (ECMRA)

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: http://www.ecmra.mil. Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year, beginning with 2013.

9.0 SECURITY REQUIREMENTS

The Government requires the Contractor to establish that applicants working for the Government under this contract are suitable for the job and are eligible for a Common Access Card (CAC) and public trust position at the appropriate level or security clearance prior to the a task order start date.

9.1 SECURITY CLEARANCE REQUIREMENTS

Contractor personnel must be able to obtain and maintain the requiring access to classified information and shall obtain the appropriate security clearance prior to beginning work on this contract or any Task Orders awarded under this contract. The Government is not responsible for processing Contractor personnel for national security clearance (SECRET). The contractor shall comply with required DMDC personnel security requirements as specified by the Cybersecurity Branch. Interim Clearances will be reviewed upon notification to DMDC Information Security Branch. It is the responsibility of the contractor Facility Security Officer (FSO) to notify DMDC immediately if there is a change in clearance eligibility.

If at any time, any contractor's FSO is unable to obtain/maintain an adjudicated Personnel Security Investigation (PSI), the Contractor shall immediately notify the DMDC Cybersecurity Branch and remove such person from work under this contract.

Overarching security requirements and Contractor access to classified information shall be as specified in the basic DD Form 254. All contractor personnel with access to unclassified information systems, including e-mail, shall have at a minimum a favorable T1. The contractor personnel shall have the required security clearance prior to arrival to perform the tasks of this contract.

Facility Security Clearance: The work performed under this contract is up to the Top Secret level and shall require Sensitive Compartmented Information (SCI) access eligibility for some personnel. The contractor shall have a final Top Secret Facility Clearance (FCL) from the Defense Security Service (DSS) Facility Clearance Branch (FCB).

Security Clearance and Information Technology (IT) Level: All personnel performing on this contract shall be U.S. citizens. Personnel security requirements will be determined at the task order level.

Investigation Requirements: All personnel requiring SCI, Top Secret or IT-I eligibility under this contract must undergo a favorably adjudicated Single Scope Background Investigation (SSBI) as a minimum investigation. The SSBI will be maintained current within 5-years and re-quests for Special Background Periodic Review (SBPR) will be initiated 90 calendar days prior to the 5-year anniversary date of the previous SSBI or SBPR.

All personnel requiring Secret under this contract must undergo a favorably adjudicated National Agency Check, Local Agency Check and Credit Check (NACLC) as a minimum investigation. The NACLC will be maintained current within 10-years and requests for Secret Periodic

9.2 CAC Requirements

Contractor personnel with access to DMDC systems or data must comply with HSPD-12 Personal Identity Verification (PIV) issuance requirements, known as the Common Access Card (CAC) for DMDC and must be CAC or PIV ready prior to beginning work on this contract:

a) All Contractor personnel must obtain/maintain a favorable FBI National Criminal History Check (fingerprint check).
b) Two forms of identity proofed identification (I-9 document).
c) Be citizens of the United States.
d) Submit a Standard Form (SF) 86 National Security Questionnaire through e-QIP that is favorably accepted by the Office of Personnel Management (OPM) for those:
    a. Who do NOT have an active security clearance
    b. Will be obtaining a position of trust through DMDC or
    c. Have NOT been favorably adjudicated within the last 24 months.
e) Background investigation has been scheduled by OPM.
f) Maintain favorable FBI National Criminal History checks and ensure completion and successful adjudication as required for Federal employment.

9.2.1 Position of Trust

All Contractor personnel with access to DMDC systems or data must comply with DoD Personnel Security Program. All persons on this contract will be designated in a Critical-Sensitive, or Non-Critical Sensitive position (IT-I or IT-II) as determined by the Government per position responsibilities.

Prior to beginning work on this contract, the contractor will complete all required personnel security requirements as specified by the Defense Human Resource Agency (DHRA), Personnel Security Office. Complete and submit a vetting application (Standard Form (SF) 86 National Security Questionnaire through e-QIP, fingerprints and proof of US citizenship) that is favorably accepted by the Office of Personnel Management (OPM) for all employees under this contract requesting a position of trust determination.

9.2.2 **Security Clearance Requirements**

All Contractor personnel requiring access to classified information will need to obtain the appropriate security clearance prior to beginning work on this contract.
DHRA/DMDC is not responsible for processing contractor personnel for national security clearance (Secret, Top Secret, Top Secret/SCI).
The contractor must comply with required DMDC personnel security requirements as specified by the Cybersecurity Division.
Interim Clearances (e.g., Interim-Top Secret, Interim-Secret) will be reviewed by DHRA Personnel Security Office.
It is the responsibility of the contractor Facility Security Officer (FSO) to notify DHRA Personnel Security Office immediately if there is a change in clearance eligibility.
If at any time, any Contractor FSO is unable to obtain/maintain an adjudicated Personnel Security Investigation (PSI), the Contractor shall immediately notify DHRA Personnel Security Office and DMDC Cybersecurity Division and remove such person from work under this contract.

9.2.3 **LAN Access Requirements:**

It is the responsibility of the Contractor to comply with account access requirements as specified by the DMDC Cybersecurity Division.

- Standard User LAN access at a minimum requires:
  a. Completed DMDC personnel security requirements.
  b. Complete DD 2875 Form(s) for all access required.
  c. Submit proof of completion for Personally Identifiable Information (PII) Training.
  d. Submit proof of completion Cyber Awareness Challenge Training.
  e. Adhere to and sign the DMDC Information Systems User Agreement(s).
- Privilege User LAN access at minimum requires:
  a. Completed DMDC personnel security requirements.
  b. Complete DD 2875 Form(s) for all access required.
  c. Submit proof of completion Privilege User Cyber Awareness Challenge Training.
  d. Adhere to and sign the DMDC Privilege Information Systems User Agreement(s).
  e. DoD 8140.01, Cyberspace Workforce Management certification.
  f. Computing Environment (CE) certification(s).

Privilege User must have Computing Environment (CE) certifications for operating system(s) Labor categories to be added		
IAT Level I	**IAT Level II**	**IAT Level III**
Computing Environment (CE)	Network Environment (NE)	Enclave Enviornment (EE)
Help Desk Support	System Adminsitrator	IT Division Chief
Local Administrator	Database Administrator	IT Director
Developer/Programmer	Network Administrator	Domain Administrator
Software Engineer	Application Administrator	Enterprise Administrator
Software Architect	Security Administrator	Backup Administrator
	Mainframe Administrator	
IAM Level I	**IAM Level II**	**IAM Level III**
Privacy Officers	Security Engineer	Cybersecurity Division Chief
Vetting Officer	Security Analysit	Cybersecurity Branch Chief
Disaster Recovery Manager	Security Auditor	Information System Security Officer
Physical Security Officer		Information System Security Manager
IASAE I	**IASAE II**	**IASAE III**
Architect	Architect Branch Chief	Chief Technology Officer
Cross Domain Solution Manager	Security Architect	Architect Division Chief
	Network Architect	Enterprise Architect

Cybersecurity Job Function Mapping to Categories and Level

9.2.4 **Cybersecurity Requirements**

9.2.4.1 The Contractor and all Contractor personnel with access to or responsibility for nonpublic Government data under this contract shall comply with DoD Instruction 8500.01 Cybersecurity, DoD Instruction 8510.01 Risk Management Framework, NIST SP 800-53 Cybersecurity Controls and Enhancements, DoD Directive 5400.11 DoD Privacy Program, DoD 6025.18-R DoD Health Information Privacy Regulation, DoD 5200.2-R Personnel Security Program, and Homeland Security Presidential Directive (HSPD) 12.

9.2.4.2 The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of government data. At a minimum, this must include compliance with DoDI 8500.01, DoDI 8510.01 and NIST SP 800-53 and provisions for personnel security and the protection of sensitive information, including Personally Identifiable Information (PII).

9.2.4.3 Contractor systems and information networks that receive, transmit, store, or process nonpublic government data must be accredited according to DoD Instruction 8510.01 Risk Management Framework (RMF) and comply with NIST SP 800-53 and annual Federal Information Security Management Act (FISMA) security control testing. All systems subject to RMF must present evidence of Assessment and Accreditation (A&A) testing in the form of an Authorization to Operate (ATO) and Cybersecurity Risk Assessment. Evidence of FISMA compliance must be presented in the form of a POA&M. The Contractor will be responsible for the cost of Cybersecurity A&A and FISMA testing required for any Contractor owned and operated network, facility and/or application processing DoD information.

9.2.4.4 The Contractor shall ensure all media containing sensitive information (e.g., hard drives, removable disk drives, CDs, DVDs) considered for disposal will be destroyed. Prior to destruction, media will be sanitized, i.e., all prudent and necessary measures shall be taken to ensure data cannot be retrieved through known conventional or unconventional means. USB Flash drive use is prohibited by DoD.

9.2.4.5 To the extent that the work under this contract requires the Contractor to have access to DoD sensitive information the Contractor shall after receipt thereof, treat such information as confidential and safeguard such information from unauthorized use and disclosure. The Contractor agrees not to appropriate such information for its own use or to disclose such information to third parties unless specifically authorized by the Government in writing.

9.2.4.6 The Contractor shall allow access only to those employees who need the sensitive information to perform services under this contract and agrees that sensitive information shall be used solely for the purpose of performing services under this contract. The Contractor shall ensure that its employees will not discuss, divulge or disclose any such sensitive information to any person or entity except those persons within the Contractor's organization directly concerned with the performance of the contract.

9.2.4.7 The Contractor shall report Cybersecurity incidents to the Cybersecurity Division.

9.2.4.8 The Contractor shall be responsible for safeguarding all government equipment, information and property provided for Contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

9.2.4.9 Contracting work performed shall be done using government provided email and resources. Resources include government furnished equipment. The Contractors company (and personal) computer shall not be used to perform to include store or transmit government work.

9.2.4.10 Final approval for all Cybersecurity tasks under this contract belongs to the Enterprise Service Directorate, Cybersecurity Division. The contractor is expected to obtain this final approval from Cybersecurity. All cybersecurity-related design, decisions, including cryptography, authentication, access control, data transfer and storage, Need-to-Know (NTK), or other IA technologies, must be coordinated with and approved by the Cybersecurity Division.

9.2.4.11 The Government may terminate this contract for default if Contractor or an employee of the Contractor fails to comply with the provisions of this clause. The Government may also exercise any other rights and remedies provided by law or this contract, including criminal and civil penalties.

10.0 CONTRACT ADMINISTRATION

This section provides roles, responsibilities, and contract administration requirements for the EITS II contract and task orders issued under it. Additional contract administration requirements will be designated at the task order level.

10.1 ORIENTATION/POST AWARD CONFERENCE

The Contractor shall participate in a Government-scheduled post-award orientation after IDIQ and task order award or in accordance with Federal Acquisition Regulation Subpart 42.5. Within 5 business days

of award the Contractor shall conduct an orientation briefing for the Government. The intent of the briefing is to initiate the communication process between the Government and Contractor by introducing key task participants and explaining their roles, reviewing communication ground rules, and assuring a common understanding of subtask requirements and objectives. The Orientation Briefing's place, date and time shall be mutually agreed upon by both parties within a week from the date of award. The completion of this briefing will result in the introduction of both Contractor and Government personnel performing work under this contract. The Contractor will demonstrate confirmation of their understanding of the work to be accomplished under this PWS.

10.2 GOVERNMENT POINTS OF CONTACT

GSA Contracting Officer (CO)
Mr. Ryan Schrank
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor, 100 S. Independence Mall West, Philadelphia, PA 19106
E-mail: Ryan.Schrank@gsa.gov
Tel: 215-446-5823

GSA Contracts Specialist (CS)
Michael Levy
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor, 100 S. Independence Mall West, Philadelphia, PA 19106
E-mail: Michael.Levy@gsa.gov
Tel: 215-446-5806

GSA Project Manager / Contracting Officer's Representative (COR)
Mr. Scott Ostrow
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor, 100 S. Independence Mall West, Philadelphia, PA 19106
E-mail: Scott.Ostrow@gsa.gov
Tel: 215-446-4497

Alternate GSA Project Manager / COR
Ms. Carol Carpenter
E-mail: Carol.Carpenter@gsa.gov
Tel: (b) (6)

DMDC Points of Contact (POC)
The name(s) and role(s) of DMDC POCs will be designated at time of award.

10.3 CONTRACT TYPE

Tasks orders issued under the EITS II IDIQ contact may be priced on a firm fixed price basis, a labor hour basis, or a hybrid firm fixed price/ labor-hour basis.

10.4 PERIOD OF PERFORMANCE

The period of performance is one (1) 12-month base plus four (4) 12-month option periods.

Option periods will be exercised at the Government's unilateral right in accordance with FAR 52.217-9 - Option to Extend the Term of the Contract (Mar 2000). The government may extend the term of this contract by written notice to the contractor within thirty (30) calendar days before the contract expires; provided that the government gives the contractor a preliminary written notice of its intent to extend at least sixty (60) calendar days before the contract expires. The preliminary notice does not commit the government to an extension. If the government exercises an option, the extended contract shall be considered to include this option clause. The total duration of this contract, including the exercise of any options under this clause, shall not exceed sixty (60) months.

10.5 LOCATION OF WORK

DMDC anticipates the majority of work performed under this effort will be by on-site personnel. However, the Contractor shall propose both on-site and off-site for consideration. Places of performance may include: DMDC facilities in both Seaside, CA and Alexandria, VA. Specific places of performance may vary during performance as required to meet government requirements. Other performance locations may be designated at the task order level.

10.5.1 TELECOMMUTING

The Government may permit telecommuting by contractor employees when determined to be in the best interest of the Government in meeting work requirements. The Contractor must have an established program, subject to review by the Government. All telecommuting agreements must be authorized and approved by the COR and include the date, time, and description of the tasks to be performed. Telecommuting will be at no additional cost to the Government. Required travel to the Government site will be the expense of the Contractor. The Contractor shall provide adequate oversight of work products to ensure contract adherence. Contractors shall have formal telework policies in place if telework is employed. Telework arrangements on individual task orders shall be approved by the Contracting Officer and the COR prior to commencement. The Contractor shall provide services from their authorized telework worksite location IAW Department of Defense Instructions (DoDI) 1035.01, Telework Policy. The Contractor shall:

- Develop, implement and operate telework programs IAW DoDI 1035.01.
- Delegate authority for telework implementation to subordinate authorities as deemed appropriate.
- Designate a Program Manager to oversee implementation of the telework program.
- Track contractor personnel participation and provide usage data to the COR at the end of each calendar year as an Annual Telework Report.
- Fully train all telework contractor personnel on the telework procedures including information technology and data security, and safety requirements consistent with:
    - the guidance in DoD Directive (DoDD), reference (g) through (j)
    - DoDD 8000.01, Management of the Department of Defense (DoD) Information Enterprise
    - DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG)
    - DoDD 8500.01E, Information Assurance (IA)
    - DoDD 5400.111, DoD Privacy Program

The Contractor shall account for and report the teleworkers time spent in the telework status in the same manner as if the employee reported for work at a traditional worksite and track teleworkers time spent in a travel mode away from the alternate worksite during a period that is scheduled for telework.

10.6 HOURS OF OPERATION

The Contractor shall perform the services required under this contract during normal business hours or after hours as may be necessary so that access to the systems may not be interrupted during normal business hours. The window for normal business hours at DMDC is between 8:00 AM and 5:00 PM EST and PST, Monday through Friday, except for Federal holidays (New Year's Day, Martin Luther King Day, Presidents Day, Memorial Day, July 4th, Labor Day, Columbus Day, Veterans Day, Thanksgiving and Christmas).

The Contractor shall be expected at work on all other days and shall provide development services at offsite locations if they are unable to enter closed government facilities.

Other hours of operation may be designated at the task order level.

10.7 TRAVEL

Travel may be required to various locations CONUS, as directed by the Government on a cost-reimbursable basis. The Contractor shall adhere to the following travel regulations (see FAR 31.205-46):
(1) Federal Travel Regulations (FTR) prescribed by the General Services Administration, for travel in the contiguous United States.
(2) Joint Travel Regulation (JTR) prescribed by the Defense Travel Management Office
(3) Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas", prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

The Contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

10.7.1 Travel Requests

Before contractor travel is executed, the Contractor shall have travel approved by, and coordinated with the COR. See Appendix O, Travel Request Form.
The Contractor's travel notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long distance travel, the Contractor shall prepare a Travel Request Form for Government review and approval. The Government shall approve all travel in writing. Long distance travel will be reimbursed for cost of travel comparable with the FTR, JTR, and DSSR.
Requests for travel approval shall:

a. Be prepared in a legible manner;
b. Include a description of the travel proposed including a statement as to purpose;
c. Be summarized by traveler;
d. Identify the travel request/travel authorization number associated with the travel;
e. Be submitted in advance of the travel with sufficient time to permit review and approval.
f. Not be considered approved until written approval is received from the COR (email shall suffice in limited circumstances).

The Contractor shall propose and utilize an organized method and format for the tracking and approval process associated with all Travel Requests. The method and format will be reviewed and approved by the COR post award.

10.7.2 **Trip Reports**

The Government will identify the need for a Trip Report (if required) when the request for travel is submitted. The Contractor shall keep a summary of all long-distance travel, to include, at a minimum, the name of the employee, location of travel, duration of trip, and POC at travel location.
Trip Reports will be fully documented within five business days of return for Government review. Trip Reports shall be provided for all conferences, IPRs, and travel, unless forbearance is granted by the GSA or DMDC COR.

10.8 GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND INFORMATION (GFP/E/I)

GFP will be identified and provided at the individual task order level. The Government will provide all Government Furnished Property (GFP) in accordance with FAR Part 45 guidelines.
Government Furnished Material (GFM) and Government Furnished Equipment (GFE) may be provided to support individual task orders under this IDIQ. Contractors shall be responsible for preventing damage to all GFM/GFE. Contractors shall be responsible for conducting all necessary examinations, inspections, maintenance and tests of all GFE. Contractors shall be responsible for reporting all inspection results, maintenance actions, losses and damage to the Government. If a Contractor loses or damages the equipment, it will be the Contractor's responsibility, in accordance with the contract clauses, to replace or repair the equipment to original or better condition at no additional cost to the Government.

Contractors shall dispose, recycle, or salvage components as directed by the Government. Contractors shall, at a minimum, meet the requirements in accordance with MIL-STD-882E and DoD 5000.02. At the conclusion of each task order PoP, the Contractor shall account for, return, and/or dispose of all GFP within thirty (30) calendar days from completion of the PoP.

10.9 GOVERNMENT FURNISHED INFORMATION (GFI)

The Contractor shall protect Government data and information, by treating the information as sensitive. Sensitive but unclassified information shall only be disclosed to those authorized personnel described in the task order. The Contractor shall keep the information confidential and use appropriate safeguards to maintain its security in accordance with minimum Federal standards. When no longer required, information shall be returned to Government control, destroyed, or held until otherwise directed by the Ordering CO. GFI will be identified and provided at the individual task order level. The Government will make available to contractors, GFI to include Government forms, publications and documents and access to manuals and materials necessary to perform work under the individual task orders.

The Contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of information is properly protected. The Contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under the task order.

Work under specific task orders may require that the Contractor's personnel to have access to Privacy Information. Contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, section 552a and applicable agency rules and regulations.

11.0 CONTRACTOR STAFFING

When hiring and assigning personnel under the contract, the Contractor shall keep in mind that the stability and continuity of the workforce are essential.

Specific task orders will identify contractor staff/FTE skillsets that are required at the start of work.

- *The Contactor is responsible for vetting the qualifications of its own applicants and is responsible for ensuring that each individual performing work holds the minimum 8570 baseline and Computing Environment (CE) certification(s) that apply to the functional role that the individual is to perform.*
- *The Contractor is responsible for verifying its own applicants have appropriate suitability determination and ensuring the proper background investigation is conducted based upon the privileged access level and functional role that the individual is to perform.*

11.1 RAMP-UP PERIOD

Work under this contract may require a ramp-up period at the initial state of the period of performance for the Contractor to recruit and hire personnel. If needed, the ramp-up period specifics shall be identified in the Contractor's proposal.

11.2 STAFFING ROSTER

The Contractor shall submit a staffing roster to the COR monthly, no later than the 15th business day of each month, segregated by task order. The staffing roster shall list the names of each employee working on the task order. The roster shall include as a minimum, the Contract Number, Contractor Name, Employee Primary User ID, Employee Last Name, Employee First Name, Current Security Classification, Work Location, Office Number, Phone Number, Primary Project Number, and Secondary Project Number for each employee. The Contractor shall notify the COR of any additions, deletions, or changes within one business day after the change(s).

11.3 CONTRACTOR IDENTIFICATION

All contractor/subcontractor personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression with members of the public that they are Government officials. Electronic mail signature blocks shall identify contractor/company affiliation. The Contractor must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed. Contractor personnel occupying collocated space in a Government facility shall identify their workspace are with their name and company/contractor affiliation.

All contractor/subcontractor personnel that have access to and use of the Government electronic mail (e-mail) shall identify themselves as contractors on all outgoing e-mail messages, including those that are sent in reply or are forwarded to another user. To best comply with this requirement, contractor/subcontractor staff shall set up an e-mail signature ("AutoSignature") or an electronic business card ("V-card") on each contractor employee's computer system and/or Personal Digital Assistant (PDA) that will automatically display "Contractor" in the signature area of all e-mails sent. All work performed shall be conducted using government provided email. Personal or company email shall not be used to perform government work.

11.4 Contractor Training

The Contactor shall provide fully trained and experienced personnel for performance under task orders awarded under EITS II. The Contractor shall train contractor personnel, at its own expense, except under rare circumstances when the CO has given prior approval for specific training to address unique, specialized requirements of the government that are peculiar to a particular task order.

11.5 Labor Categories

The EITS II Basic Contract includes the standard set of labor categories. The Contractor's standard labor categories and labor rates included in the EITS II Basic Contract's Pricing Template are hereby incorporated by reference and made a material part of this contract.

11.5.1 Key Personnel

Key personnel are those personnel considered essential to successful Contractor performance.
As a minimum, the Corporate IDIQ Contracts Manager and Corporate Program Manager Key Personnel shall be available at contract start.

The contractor shall designate on-site managers to provide management, administrative, and technical interface with the COR in accomplishing services under this contract. The Contractor shall provide managers that are knowledgeable and experienced in management of all aspects of communications within their designated Area of Responsibility (AOR). These individuals shall be available on a part-time basis during contract transition and full-time by the contract start date.

The Contractor is expected to minimize employee turnover with respect to personnel performing under this Task Order. The Contractor shall not remove or replace any personnel designated as key personnel under this TO without the written concurrence of the CO. Prior to utilizing other than personnel specified in the task order proposal submitted in response to this requirement, the Contractor shall notify the Government CO and the COR. This notification shall be no later than ten (10) calendar days in advance of any proposed substitution and shall include a resume for the proposed substitution and justification in sufficient detail to permit evaluation of the impact of the change on TO performance.

The request shall be written and provide a detailed explanation of the circumstances necessitating the proposed substitution. The Contractor shall submit a resume for the proposed substitute and any other information requested by the COR needed to approve or disapprove the substitution. The COR will evaluate such requests and promptly. The replacement key personnel shall possess skills of equal or greater qualifications to those being replaced. The CO will notify the Contractor of approval or disapproval thereof in writing.

If the Government CO and the COR determine that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the substitution will be denied and the Contractor shall propose an alternate candidate.

If a key personnel position on a Task Order is vacant for more than 14 calendar days, the associated hours for this position starting at day 15 will be deducted from the invoice. This will apply to both Firm Fixed Price and Labor Hour task orders.

11.5.2 **Corporate Key Positions**
The Contractor shall assign a Corporate IDIQ Program Manager and Corporate IDIQ Contracts Manager to represent the Contractor as primary points of contact to perform Basic Contract level duties, resolve issues and related functions associated with the contract and task orders solicited and awarded under the EITS II IDIQ Contract.

No costs for the Corporate IDIQ Program Manager, the Corporate IDIQ Contracts Manager may be billed to the Basic Contract.

11.5.2.1 **Corporate IDIQ Contracts Manager**
The Contractor shall provide a Contracts Manager who shall be responsible for the contractual administration of the contract.

11.5.2.2 **Corporate IDIQ Program Manager**
The Contractor shall provide a Program Manager (PM) who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the Contractor when the PM is absent shall be designated in writing to the KO within 24 hours of contract award. The PM or alternate shall be available between the hours of 07:30 16:30 PST.

11.5.2.3 Mandatory Key Personnel Position Descriptions
The following Contractor personnel are essential for successful accomplishment of the work to be performed under the resultant contract and are defined as Key Personnel. The Government anticipates needing Key Personnel at the task order Level depending on the complexity of the requirements. The Government may require that these positions to be staffed in a full-time capacity for the duration of each order concurrently for multiple Task Orders.

All costs associated with the Contractor Key Personnel positions listed below shall be handled in accordance with the contractor's standard accounting practices:

11.5.2.3.1 Quality Assurance (QA) Manager
Candidate must be knowledgeable of SDLC methodologies and industry best practices such as the IEEE Standard 1012-2004 for Software Verification and Validation and SEI CMMI level 3 procedures and processes.

11.5.2.3.2 Senior Enterprise Architect (EA)
Candidate shall have a bachelor's degree in information technology or related field (e.g., Federated Enterprise Architecture Certification), and relevant senior level work experience with enterprise architecture and CompTIA Security+.

11.5.2.3.3 Senior Database Engineer
Candidate shall have a bachelor's degree in information technology or related field Database architecture and design experience in planning and implementing large-sized database and cloud database technology.

11.5.2.3.4 Senior Software Engineer (SSE)
Candidate shall have a bachelor's degree in information technology or related field. Candidate shall have advanced technical expertise and shall have performed as a technical lead responsible for the development of solutions. The SSE shall have the ability to manage the entire software development lifecycle.

11.5.2.3.5 Senior Information Security Analyst
Candidate shall have a bachelor's degree in information technology or related field. Candidate shall have significant experience with DoD's RMF, DIACAP, NIST Certification & Accreditation and possess a DoD Security+ or CISSP Certification.

11.5.3 **Unique Professional Skills**
Unique professional skills are defined as those bona fide executive and highly specialized skills for which the expertise required or duties performed are within the EITS II Contract's scope, but are so specialized or rare that they are not explicitly defined in any of the EITS II standard labor category descriptions. If a unique need arises, the NPA may propose a specialized labor category outside of the labor categories established in the EITS II Contract. The contractor shall submit an explanation justifying the need for this specialized skillset. The contractor shall comply with all the applicable contract clauses and labor laws, including the Service Contact Act or the Davis Bacon Act, as applicable.

The GSA Contracting Officer will determine whether circumstances warrant use of unique professional skills. Based on price or cost analysis, the GSA Contracting Officer will negotiate a fair and reasonable labor rate with the Contractor at the task order level.

11.5.4 **Technical Refreshment**
After contract award, the Government may implement technical refreshment of the scope and/or the labor categories consistent with FAR 52.212-4 in order to improve performance or react to changes in technology.

11.6 Subcontracting
In accordance with FAR 52.219-9, the Contractor shall provide a subcontracting plan for Contracting Officer review and approval. After approval of the subcontracting plan, the Contractor shall not enter into additional subcontract agreements without approval of the Contracting Officer and the Contracting Officer representative. The Contractor will be notified within five (5) business days by the Contracting Officer whether the subcontractors has been approved or disapproved. All subcontracts shall include the identity of the subcontractor, the extent of the work, and the reason for subcontracting. Please reference FAR clause 52.244-2.

11.6.1 **Subcontracting Considerations**
EITS II prime NPA(s) are responsible for managing the workload mix being performed under their contract(s) and Orders.

EITS NPA(s) are expected to perform a meaningful amount of work/add significant readily-identifiable value on each Order to prevent pass-through situations. This is an area of increasing regulation, as evidenced by the DoD interim rule for pass throughs cited in GAO report GAO-08-269, January 25, 2008, and as identified in Section 866 of the Duncan Hunter National Defense Authorization Act of 2009, P.L. 110-417 ("DHNDAA" or "NDAA 2009").

It is a best practice for GSA Contracting Officers to require industry partners to disclose the amount of work they intend to perform with their own resources in Order RFQs and RFPs. The GSA Contracting Officer may require Order invoice level subcontracting reporting should they wish to monitor these matters closely during Order performance.

It is reasonable and routine that on larger tasks, contractors may manage capacity building through subcontracting with small business firms and other than small business firms to provide scalability in the early stages of performance or during increases of work to be performed. It is reasonable to consider the total prospective life cycle of an order, including option periods, when evaluating how much work the prime plans to perform for a given task order. The GSA CO may request a well-defined plan from NPA prime contractors to facilitate this review, and may qualitatively evaluate such plans during task order evaluation if required under the task order solicitation.

11.7 Cooperation With Other On-Site Contractors

When the Government undertakes or awards other orders or contracts for additional work the Contractor will: (1) fully cooperate with the other Contractors and Government employees, and (2) carefully fit its own work to such other additional contracted work as may be directed by the COR. The Contractor shall not commit or permit any act that will interfere with the performance of work awarded to another Contractor or with the performance of other Government employees. In any case where, in the course of fulfilling the order requirements, the Contractor disturbs any work guaranteed under another separate contract, the Contractor shall restore such disturbed work to a condition satisfactory to the COR and guarantee such restored work to the same extent as it was guaranteed under the other contract.

12.0 APPENDICES

Appendix A.1 - EITS II Portfolio
Appendix A.2 - Overview of DMDC Major Programs
Appendix B - DMDC IT environment Overview
Appendix C - DMDC Computing Environments
Appendix D - SDLC - Process Handbook
Appendix E - Release Manager Charter
Appendix F - Enterprise DBA Standard Operating Procedure (SOP)
Appendix G.1 - Configuration Management Policy
Appendix G.1 - Configuration Management Handbook
Appendix H - Development Steering Group Charter
Appendix I - Quality Assurance Testing Guidelines
Appendix J - Incident Management Service Restoration Team (SRT) Standard Operating Procedure (SOP)
Appendix K - DMDC Information Assurance Policy
Appendix L - Cyber Security Common Language
Appendix M - DD 254
Appendix N - DMDC Senior Management Review Format
Appendix O - Travel Request Form
Appendix P - Quality Assurance Surveillance Plan
Appendix Q - Performance Requirements Summary
Appendix R - Problem Notification Report (PNR) Template
Appendix S - Contract Discrepancy Report (CDR) Template
Appendix T - CPARS Form and Ratings Definitions
Appendix U - EITS II Labor Categories & Labor Category Descriptions *(included in Price Template)*
Appendix W- EITS II Nondisclosure Agreement